

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-254543

(43)Date of publication of application : 06.11.1987

(51)Int.Cl.

H04L 9/00
// G06F 15/30

(21)Application number : 61-096705

(71)Applicant : HITACHI LTD

(22)Date of filing : 28.04.1986

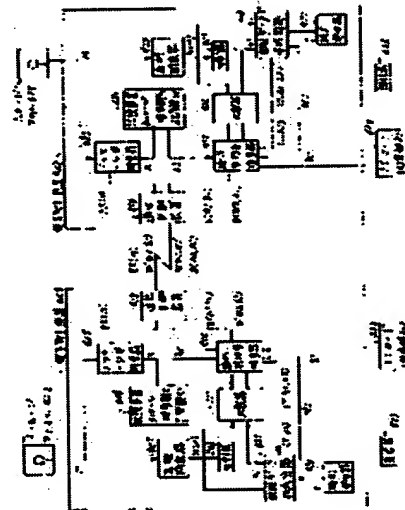
(72)Inventor : TAKARAGI KAZUO
KURASHIKI NOBUHIRO
SASAKI RYOICHI
SHIRAISHI TAKAYOSHI

(54) ELECTRONIC TRANSACTION SYSTEM

(57)Abstract:

PURPOSE: To prevent a verifying personnel from running away with an electronic signature of a signer by devising a digital signature in such way that a specific condition is to be satisfied.

CONSTITUTION: The identification of the concerned personnel is checked twice by executing the confirmation of sender/recipient, addition of certification of contents, provision of pass code and the fact of reply of a terminal equipment as procedures of the transaction. Then the additional verification personnel of a tally impression sending procedure from the verification personnel to a signer receives a message M from the signer, confirms the content of the message M and approves of the transaction. In this case, the fact that a high-order bit string h1 in a compressed ciphered text of the message M is included in the tally impression generated by the verification personnel only is to be confirmed. Thus, the fact is used for a proof if the verification personnel negates the existence of the transaction at the exchange of the electronic signature, does not reply the electronic signature of the verification personnel as a reply and runs away with the electronic signature of the signer.



LEGAL STATUS

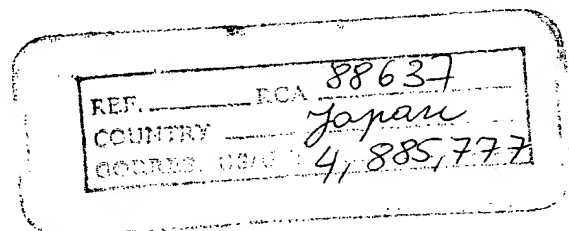
[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]



[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭62-254543

⑬ Int.Cl.⁴
H 04 L 9/00
// G 06 F 15/30

識別記号

330

庁内整理番号

A-7240-5K
7208-5B

⑭ 公開 昭和62年(1987)11月6日

審査請求 未請求 発明の数 1 (全10頁)

⑮ 発明の名称 電子取引方式

⑯ 特 願 昭61-96705

⑰ 出 願 昭61(1986)4月28日

特許法第30条第1項適用 昭和60年11月5日 社団法人電子通信学会発行の「昭和60年度電子通信学会情報・システム部門全国大会講演論文集」に掲載

⑱ 発 明 者 宝 木 和 夫 川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑲ 発 明 者 倉 敷 信 宏 東京都渋谷区道玄坂1丁目16番3号 株式会社日本ビジネスコンサルタント内

⑳ 発 明 者 佐々木 良一 川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

㉑ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

㉒ 代 理 人 弁理士 小川 勝男 外1名
最終頁に続く

明 細 書

1. 発明の名称

電子取引方式

2. 特許請求の範囲

1. 書類を電気的情報に置き換えて、電子的に所望の取引を行う電子取引方式において、

予め、取引文を非正式に認めたことを示す認証データを作成する第1の認証データ作成方法と、取引文を正式に認めたことを示す認証データを作成する前記第1の認証データ作成方法とは異なる第2の認証データ作成方法を定めておき、第1の取引者(甲とする)と第2の取引者(乙とする)が取引を行う場合に、

甲は、該取引文に対し、第1の認証データ作成方法により、第1の認証データを作成して乙に送信し、乙は、甲より該第1の認証データを受信した後に、該取引文に対し、第2の認証データ作成方法により第2の認証データを作成して甲に送信し、

甲は、乙より該第2の認証データを受信した

後に、該取引文に対し、第2の認証データ作成方法により第3の認証データを作成して乙に送信することにより、該取引を成立させることを特徴とする電子取引方式。

2. 前記第1の認証データ作成方法は、予め定められた公開鍵暗号方式を用い、取引の状況を示す第1の取引状況データを秘密鍵で暗号化してその暗号文を認証データとする方法であり、前記第2の認証データ作成方法は、予め定められた公開鍵暗号方式を用い、前記第1の取引状況データとは異なる第2の取引状況データを秘密鍵で暗号化してその暗号文を認証データとする方法であることを特徴とする第1項記載の電子取引方式。

3. 前記第1の取引状況データは、該取引文を第1の圧縮暗号化方法により圧縮暗号化した第1の圧縮暗号文を含んでおり、かつ、第2の取引状況データは、該取引文を前記第1の圧縮暗号化方法とは異なる第2の圧縮暗号化方法により圧縮暗号化した第2の圧縮暗号文を含んでいる

特開昭62-254543 (2)

ことを特徴とする第1項記載の電子取引方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、書類をコンピュータのメッセージに置き換え、電子的に商取引を行う電子取引方式に関する。

〔従来の技術〕

従来より、契約交渉はサイン、印鑑によりその正当性を認証している。利害関係にあるデータが電子取引のように通信でやりとりされる場合、サイン、印鑑データをそのままデジタル通信に変換して送っても、簡単にコピーされる恐れがあり、認証には使用できない。そこで、通常のサイン、印鑑に相当するデジタル署名が必要になる。ここで、メッセージ認証が署名として有効になるためには、次の3条件を満足しなければならない。

- (1) 通信文が第三者によって偽造できない。
- (2) 受信者が後で、(a) 受信の事実を否定したり、(b) 受信文を偽造したりできない。

容易にデジタル署名が実現できる。

第2図に公開鍵暗号によるデジタル署名のフローチャートを示す。

ステップ101では、送信者AからのメッセージMを入力する。

ステップ102では、メッセージMを送信者Aの秘密鍵S1で復号化した復号文D(M, S1)を作成する。

ステップ103では、復号文D(M, S1)をさらに受信者Bの公開鍵R2で暗号化して、暗号文L=E(D(M, S1), R2)を得て、これを受信者B宛に送信する。

ステップ104では、受信者B宛の受信データLを受信者Bの秘密鍵R1で復号化してD(M, S1)を得る。

ステップ105では、復号文D(M, S1)を送信者Aの公開鍵S2で暗号化してもとのメッセージMを求める。

ステップ106では、メッセージMを受信者Bに出力データとして出力する。

- (3) 送信者が後で、(a) 送信の事実を否定したり、(b) 送信文を偽造したりできない。

デジタル署名を実現する手段として次の方法が提案されている。

- (1) 慣用暗号を用いたデジタル署名
- (2) 公開鍵暗号を用いたデジタル署名
- (3) ハイブリッド方式によるデジタル署名

次に上記3方法の特徴と問題点を述べる。

(1) 慣用暗号を用いたデジタル署名

一般にDES方式の暗号を用いたデジタル署名がいろいろ提案されているが、公証機関が必要であったり、送信側と受信側で共通の認証鍵を持つため受信者が署名文を改ざんすることができるという問題がある。このため実用性のある署名方式はまだない。

(2) 公開鍵を用いたデジタル署名

RSAの暗号方式等を用いることにより比較的

このフロー・チャートにおいて、ステップ104では、暗号文Lは秘密鍵R1を知らないと解読できない。つまり、R1を知っているのは受信者Bだけである。また、ステップ102において、D(M, S1)を作れるのは秘密鍵S1を知っている送信者Aだけである。したがって、メッセージMを送信したのは確かにAであり、メッセージを受け取ったのは確かにBであるということになる。

さらに、メッセージMが、通常の文章ではなくランダムなデータであったりした時には、Mが正當なものかどうか判定しにくい。この対策としてメッセージに送信者の識別名、受信者の識別名、メッセージの通し番号、日付等の付属情報を付けて送信することができる。これにより、署名文をコピーして何度も送るような不正行為を防止することができる。

しかし、RSAによる方式では、演算が複雑になるため暗号化、復号化に時間がかかり、メッセージが長い場合には問題になる。

特開昭62-254543 (3)

(3) ハイブリッド方式によるデジタル署名

この方式は、DESの暗号方式の利点とRSAの暗号方式の利点をうまく利用しそれぞれの方法をミックスさせたものである。

通常のメッセージはDESによる暗号通信で送信し、鍵の配送と認証はRSAの方式を使っている。認証の対象となるメッセージは、先ず、DESによるデータ圧縮型暗号化処理を行いハッシュ・トータルを求める。第3図にこの方法を示す。第3図において、次の処理を行う。

ステップ201:

入力メッセージMの先頭から56ビット単位でn個に分割し、先頭からM1, M2, ..., Mnとする。

$$M = M1, M2, \dots, Mn$$

ステップ202:

Mi (i = 1, 2, ..., n) に7ビット単位で1ビットのパリティ・ビットを付加し、それを

前記データ圧縮型暗号処理により短い文字列

303 (圧縮型暗号文 = H(M)) を算出し、秘密鍵304 (k1) を用いて暗号機305によりデジタル署名306 (E(H(M), k1)) を作成して、受信者307へ送信する。受信者307がメッセージ302と署名306が、真性のものであると認めるためには、送信者301の公開鍵308 (k2) を用いて、デジタル署名306を暗号機309により復号化して元の文字列

310 (H(M')) を作成するとともに、送信者301と同様の方法でメッセージ302から文字列311 (H(M')) を算出する。そうして、この両者をブロック312で比較し、結果が一致すれば、送信者301が秘密鍵304の唯一の所有者であると信じる限りは、メッセージ302は真性である。

この方式では、長いメッセージに対するデジタル署名でも、短時間で処理できる。

〔発明が解決しようとする問題点〕

以上述べてきた従来方式は、デジタル署名の

Ki (i = 1, 2, ..., n) とする。

ステップ203:

j = 1, 2, ..., nとして、以下の処理を繰り返す。

・ Kj を暗号化鍵として、I (j-1) を暗号化し、その暗号化結果とI (j-1) との排他的論理和をとり、その結果をI (j) とする。

$$I(j) \leftarrow I(j-1) \oplus EK_j(I(j-1))$$

(但し、I (0) は、初期値。)

ステップ204:

$$H(M) = I(n)$$

最後に得られた暗号ブロック圧縮暗号文H(M)に、RSA方式によるデジタル署名を行う。

次に第4図により、ハイブリッド方式によるデジタル署名の方法を示す。

送信者301は、メッセージ302 (M) から

条件である(2)-(a)「受信者が後で、受信の事実を否定できない。」を満足していない。つまり、受信者は事後において、そのような受信の事実はないと主張した場合、送信者はそれを否定する証拠を持たない。

本発明の目的は、デジタル署名におけるこのような従来の欠点を除去したうえで、次の条件を満足する電子取引を実現することにある。

- (1) 通信文が第三者によって偽造できない。
- (2) 受信者が後で、(a) 受信の事実を否定したり、(b) 受信文を偽造したりできない。
- (3) 送信者が後で、(a) 送信の事実を否定したり、(b) 送信文を偽造したりできない。

〔問題点を解決するための手段〕

上記目的を達成するため、本発明では次の手順を該取引において実現する。

1. 送受信者の確認
2. 内容証明機能の付加

特開昭62-254543 (4)

3. 秘密鍵の保持と端末応答の事実により、本人であることの二重チェックを行う。

以上1. ~ 3. の詳細については、特開昭60-193735号を参照されたい。

4. 認証者から署名者への割印送信手順の追加
認証者は、署名者よりメッセージMを受信し、メッセージMの内容を確認して、取引に合意する場合、予め定められたデータI₀にたいする圧縮暗号文H(M)を作成し、さらに、H(M)を上位側ビット列h₁と下位側ビット列h₂に分割(△H(M) = (h₁, h₂))して、この上位ビット列h₁と時刻データTを繋げて、割印認証用データ(T, h₁)を作成する。また、異なるハッシュ関数H₁とH₂に対し、H₁(M)とH₂(M)を作成し、h₁ = H₁(M)、h₂ = H₂(M)としてもよい。該割印認証用データを認証者の秘密鍵R₁で暗号化し、電子割印D((T, h₁), R₁)を作成し、これを署名者に該メッセージMについての取引を行うことへの合意の応答として、署名者

へ送信する。署名者は、前記電子割印D((T, h₁), R₁)を認証者の公開鍵R₂で暗号化して、元の割印認証用データE(D((T, h₁), R₁), R₂) = (T, h₁)を得る。

〔作用〕

認証者にしか作成できない割印の中にメッセージMの圧縮暗号文の上位ビット列h₁が含まれている事実を確認することにより、この後の電子捺印の交換時に認証者が、取引の事実を否定し、認証者の電子捺印を応答として返さずに署名者の電子捺印を持ち逃げした場合の証拠とすることができ。

〔実施例〕

第1図は本発明を実施するシステムの一構成例である。

第5図は、第1図の構成において本発明を実施する処理手順を示すフローチャートである。

次に、第4図における各構成要素の動作を第5図のフローチャートに従って述べる。

ステップ501: 署名者401は、メッセージ

・ファイル402より取引文Mを署名者側電子取引装置404に入力するとともに、ICカード403により自分の秘密鍵S₁と署名者401の名前、認証者426の名前を入力する。

ステップ502: 署名者側電子取引装置404は、メッセージ用暗号器405と記憶装置406のメッセージ暗号鍵Kを用いて取引文Mを暗号化したEK(M)を作成し、EK(M)と署名者401の名前、認証者426の名前を通信制御装置413により認証者側電子取引装置423に送信する。

ステップ503: 署名者側電子取引装置404は、圧縮暗号器407により取引文Mを暗号鍵として用い、次のように圧縮暗号文H(M)の作成を行う。

(1) H(M)は、64ビットの長さの入力データ(初期値)I(0)を64ビットの長さの暗号鍵K₁で圧縮暗号化した64ビットの長さの出力データである。この暗号方式は、予め定められているとする。また、この暗号方式は、入力データ

I(0)と出力データH(M)があたえられたとき、それらの2つのデータから暗号鍵K₁を求めることは、計算量的に困難なものであるとする。

(2) 取引文Mを56ビット長のブロックに区切り、各ブロックをM₁, M₂, ..., M_nとする。最後のブロックM_nの長さが56ビットに満たないときは、ビット"0"を残りの箇所に追加して、M_nの長さを56ビットとする。

(3) 前記ブロックに対して、7ビット単位で1ビットのパリティ・ビットを付加し、ブロックの長さを64ビットに拡張する。拡張された各ブロックをK₁, K₂, ..., K_nとする。

(4) 入力データI(i-1)を鍵K_iで暗号化したものとI(i-1)との排他的論理和をとったものをI(i)とする。

$$I(i) = I(i-1) + EK_i(I(i-1))$$

以上の処理をi = 1, 2, ..., nについて行う。また、初期値I(0)は、予め定められた値だと

特開昭62-254543 (5)

する。

(5)(4)で最終的に求められた値 $I(n)$ を $H(M)$ とする。また、 $H(M)$ を上位と下位のデータに分割し、それぞれを $h1$ 、 $h2$ とする。

$$H(M) = (h1, h2) = I(n)$$

ステップ504：認証者側電子取引装置423は、メッセージ用暗号器422と暗号鍵 K を用いて暗号文 $EK(M)$ を復号化する。

$$M = DK(EK(M))$$

そして、取引文 M を認証者426に知らせる。

なお、暗号器を復号器として使うためには、RSA方式では鍵を変えればよく、DES方式ではモード指定用スイッチを切り換えればよいので、以下の説明では復号器の場合も単に暗号器と記述する。

ステップ505：認証者426は、ステップ

式により、秘密鍵 $R1$ を用いて割印認証用データ $W1$ を捺印・割印用暗号器415により復号化し、 $D(W1, R1)$ を作成する。そして、 $D(W1, R1)$ を署名者側電子取引装置404に送信する。

ステップ509：署名者側電子取引装置404は、記憶装置406の認証者公開鍵 $R2$ を用いて $D(W1, R1)$ を捺印・割印用暗号装置412により暗号化し $W1' = E(D(W1, R1), R2)$ を得る。もし、秘密鍵 $R1$ と公開鍵 $R2$ が正しい暗号鍵と復号鍵の組であるなら、 $W1 = W1'$ すなわち、 $T = T'$ 、 $h1 = h1'$ が成立することになる。暗号化結果 $W1'$ を比較器411によりチェックして、その結果をディスプレイ装置(図示せず)上に表示する。もしも、 T' が予め定められた形式に合致するものであり、 $h1'$ が503で作成した $h1$ と等しいことを示す表示があれば、認証者426本人は確かに認証者側電子取引装置423に在ることを確認する。今の場合、 T' の内容は T と同じ「昭和60年4月11日15時53分12秒」となるので、上記の確認が

504により復号化された取引文 M を見て、取引をしても良いと判断したら、ICカード424により自分の秘密鍵 $R1$ を入力する。

ステップ506：認証者側電子取引装置423は、ステップ503と同様の方法により、圧縮関数器420を用いて取引文 M を圧縮暗号化し、 $H(M) = (h1, h2)$ を作成する。また、予め定められた形式に従ったデータを識別記号 T として時刻発生器417により作成する。今の場合、識別記号 T として、その時の時刻、例えば、「昭和60年4月11日15時53分12秒」を作成する。

ステップ507：該識別記号 T と分割器419により暗号データ $H(M)$ から作成した上位データ $h1$ により、割印認証用データ $W1$ を認証データ作成回路418を使って作成する。

$$W1 = (T, h1)$$

ステップ508：予め定められた公開鍵暗号方

なされる。

ステップ510：署名者401は、認証者側電子取引装置423に、確かに認証者426本人がいて、かつ、認証者426は取引文 M に対して取引を受け付けても良いと判断したことを知る。そして、自分の電子捺印を作成するため、署名者側電子取引装置404のキーボード(図示せず)上に設けた「捺印OKボタン」を押す。

ステップ511：署名者側電子取引装置404は、認証データ作成回路409に503で作成した $(h1, h2)$ と509で得た T' を入力して、捺印認証用データ $W2$ を作成する。

$$W2 = (T', h1, h2)$$

ステップ512：予め定められた公開鍵暗号方式により、秘密鍵 $S1$ を用いて割印認証用データ $W2$ を捺印・割印用暗号器412により復号化し、 $D(W2, S1)$ を作成する。そして、 $D(W2, S1)$ を認証者側電子取引装置423に送信する。

特開昭62-254543(6)

ステップ513: 認証者側電子取引装置423は、記憶装置421の署名者公開鍵S2で $D(W2, S1)$ を暗号化した $W2'$ を捺印・割印用暗号器415により作成する。

$$W2' = E(D(W2, S1), S2)$$

$W2' = (T', h1', h2')$ としたとき、比較器416により、

$$T' = T, \text{ かつ } (h1', h2') = (h1, h2)$$

が成立しているか、確認を行い、その結果を表示して認証者426に知らせる。

ステップ514: 認証者426は、ステップ513の結果が、「 $T' = T$ 、かつ $(h1', h2') = (h1, h2)$ 」が成立であることを確認したとき、 $D(W2, S1)$ は確かに署名者401本人が取引文Mに基づいて作成したものであると判断し、自分も電子捺印を作成、送信する。

$$W2' = E(D(W2, R1), R2)$$

$W2' = (T', h1', h2')$ としたとき、比較器411を用いて、

$$T' = T, \text{ かつ } (h1', h2') = (h1, h2)$$

が成立していれば、 $D(W2, R1)$ は確かに認証者426本人が取引文Mに基づいて作成したものと判断する。

ステップ518: 署名者側電子取引装置404は、取引文M、署名者401の電子捺印 $D(W2, R1)$ 、認証者426の電子捺印 $D(W2, S1)$ 、割印 $D(W2, R1)$ をメッセージファイル402に記録し、動作を終了する。

ステップ519: 署名者401は、メッセージファイル402を保管する。

ステップ520: 認証者側電子取引装置423

ことを決定する。そして、認証者側電子取引装置423のキーボード(図示せず)上に設けた電子捺印作成・送信ボタンを押す。

ステップ515: 認証者側電子取引装置423は、506で作成した $(h1, h2)$ とTから、捺印認証用データW2を認証データ作成回路418により作成する。

$$W2 = (T, h1, h2)$$

ステップ516: 認証者側電子取引装置423は、ICカード424による認証者秘密鍵R1を用いて公開鍵暗号方式により、W2を復号化した $D(W2, R1)$ を捺印・割印用暗号器415により作成する。そして、 $D(W2, R1)$ を署名者側電子取引装置404に送信する。

ステップ517: 署名者側電子取引装置404は、記憶装置406の認証者公開鍵R2を用いて、公開鍵暗号方式により $D(W2, R1)$ を暗号化した $W2'$ を捺印・割印用暗号器412により作

成する。取引文M、署名者401の電子捺印 $D(W2, S1)$ 、認証者426の電子捺印 $D(W2, R1)$ 、割印 $D(W2, R1)$ をメッセージファイル425に記録後、動作を終了する。

ステップ521: 認証者426は、メッセージファイル425を保管する。

実施例の変形例1.

前記実施例のステップ501およびステップ505において、予め、秘密鍵の一部の情報を磁気カードまたはICカードに記録しておき、秘密鍵の残りの情報を暗証番号の形で当事者が記憶しておき、秘密鍵S1、R1を入力する場合には、磁気カードまたはICカードからの情報を読み出しと暗証番号のキー入力により秘密鍵S1、R1の入力を実現しても良い。

実施例の変形例2.

前記実施例のステップ501、505、510、514のいずれかにおいて、当事者が入力操作を行う前に声紋、指紋等によって本人であることを確認する動作を該当の端末動作に追加しても良い。

特開昭62-254543 (7)

〔発明の効果〕

本発明によれば、次の条件を満足する電子取引を仲介機能の介在なしにおこなうことができる。

- (1) 第三者は、署名者又は認証者を装って不正に取引をおこなうことはできない。
- (2) 認証者は取引文を改ざんできない。
- (3) 署名者は、取引成立後、取引文の内容を否定することはできない。

これは、前記(2)で認証者が取引文を改ざんできなかったのと同様の理由による。

- (4) 認証者は、署名者の電子捺印を持ち逃げすることはできない。

次の(a)により、認証者が署名者の電子捺印を持ち逃げすることはできない。

(a) 割印の保持チェック

$$D(W1, R1') = D(W1, R1)$$

となるような、秘密鍵 $R1'$ を作成することが、計算量的に困難なため、該取引文 M による圧縮暗号文の上位側データを含む割印を作成できるのは、秘密鍵 $R1$ を持つ認証者だけである。

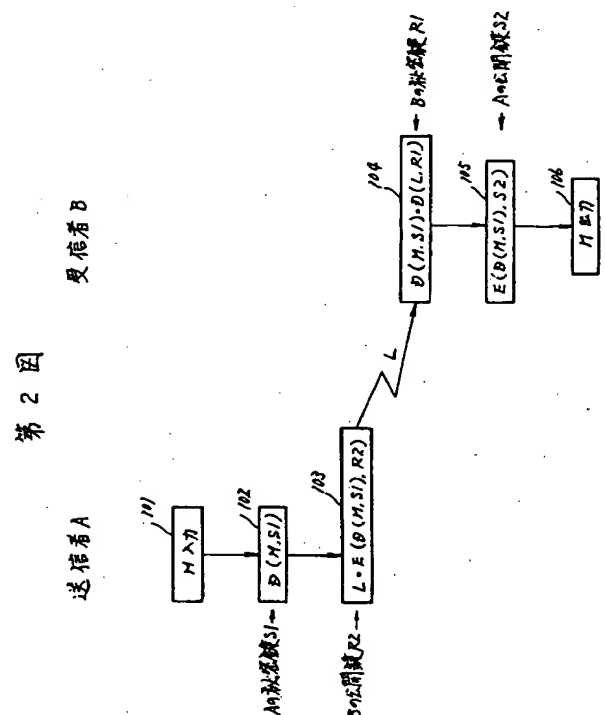
4. 図面の簡単な説明

第1図は発明を実施する一構成例を示す図、第2図は公開鍵暗号方式を用いた従来のデジタル署名方式を示す図、第3図はデータ圧縮型暗号の原理を示す図、第4図はハイブリッド方式によるデジタル署名の方法を示す図、第5図は本発明の処理手順を示すフローチャートであり、本発明を実施する場合における第1図の各構成要素の動作を記述したものである。

署名者と認証者が、取引文 M についての電子取引を行っているとき、署名者が、署名者の電子捺印 $D(W2, R1)$ を送信した後、認証者が、認証者の電子捺印 $D(W2, R1)$ を送信せず此の取引があったことを否定しようとした場合、署名者は、前記割印を認証者の公開鍵 $R2$ で復号化して、その内容をチェックすることで、認証者が取引の事実を否定して、署名者の電子捺印を持ち逃げしようとしたことの証拠とすることができる。電子捺印の交換に先立ち、認証者が、署名者に送信した割印 $D(W1, R1)$ の内容には、署名者が送信した取引文 M を圧縮暗号化して作成した $H(M) = (h1, h2)$ の上位側データ $h1$ がある。

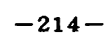
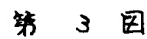
$$W1 = (T, h1)$$

第三者が認証者を装って、不正な取引を行えなかったのと同じ理由により、



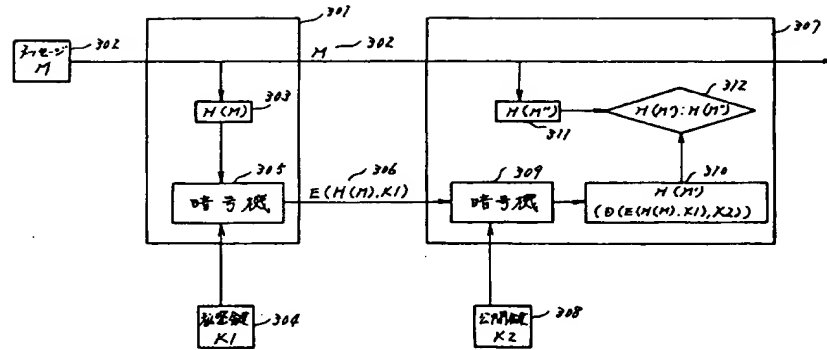
代理人 井理士 小川勝男

第 1 圖

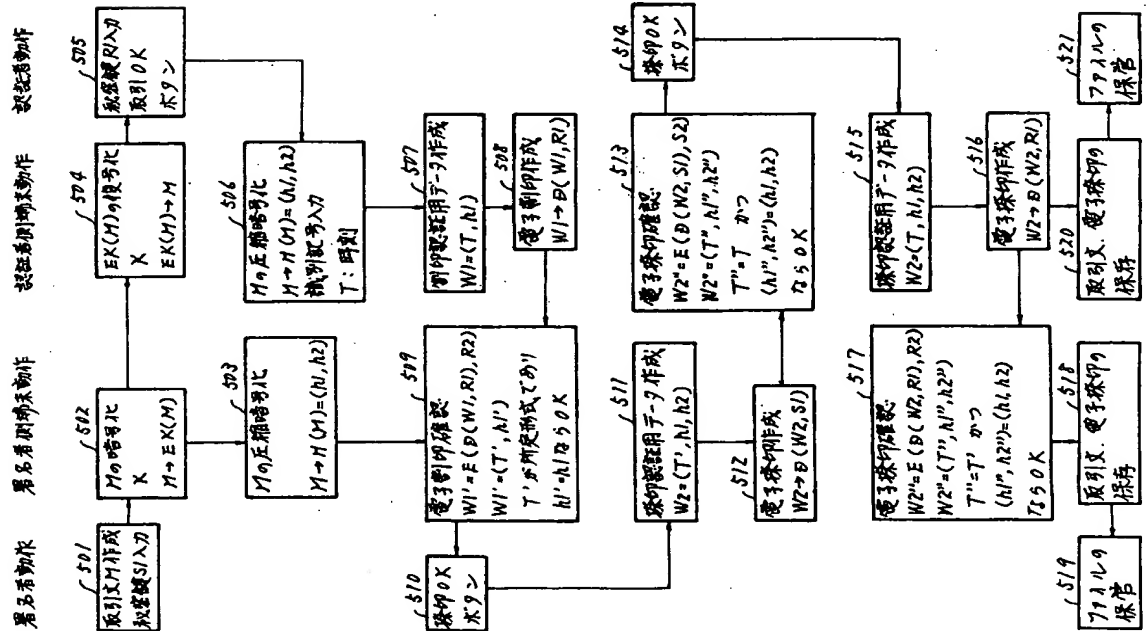


特開昭62-254543 (9)

第4図



第5図



第1頁の続き

⑬発 明 者 白 石 高 義 川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内